



## JOINT INTELLIGENCE BULLETIN



24 December 2014

**(U//FOUO) November 2014 Cyber Intrusion on USPERI and Related Threats****(U) Scope**

(U//FOUO) This *Joint Intelligence Bulletin* (JIB) is intended to provide information on the late-November 2014 cyber intrusion targeting USPERI and related threats concerning the planned release of the movie, "The Interview." Additionally, these threats have extended to USPER2—a news media organization—and may extend to other such organizations in the near future. This JIB is intended to support the activities of the FBI and DHS to assist federal, state, and local government cyber, counterterrorism, and law enforcement officials, first responders, and private sector security partners in effectively deterring, preventing, preempting, or responding to cyber and terrorist attacks against the United States.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

(U) This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label <sup>USPER</sup> and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at [IA.PM@hq.dhs.gov](mailto:IA.PM@hq.dhs.gov), [IA.PM@dhs.gov](mailto:IA.PM@dhs.gov), or [IA.PM@dhs.ic.gov](mailto:IA.PM@dhs.ic.gov).

**(U) Overview**

(U) In late November 2014, a group calling itself the Guardians of Peace (GOP) claimed responsibility for an intrusion on USPER1 and subsequently issued threats to USPER1, its employees, and theaters planning to show the movie, "The Interview."

(U) The intrusion into USPER1's network consisted of the deployment of destructive malware and the theft of proprietary information, as well as employees' personally identifiable information and sensitive business communications.

**(U//FOUO) Threats Related to the Planned Release of the Movie, "The Interview"**

(U//FOUO) Recently, GOP actors promised to deliver a "Christmas present" if USPER1 releases the movie, "The Interview." Following the 16 December implied threats of physical attacks against the theaters, major movie theater chains, followed by USPER1, cancelled plans to release the movie on 25 December 2014.

- » (U) On 13 December, a Pastebin post by GOP indicated the group was preparing to provide a "Christmas gift" of large amounts of data. The post provides e-mail accounts that should be contacted for the data.
- » (U) On 14 December, a Pastebin post provided the same message from 13 December and an additional message to USPER1 and its employees threatening more harm if GOP demands were not met.
- » (U) On 16 December, the GOP uploaded a Pastebin post that contained a message that specifically mentioned the events of 11 September 2001. It further states that people should keep their distance from locations showing the movie, including the premiere in New York City. It further encouraged people who live in areas where the movie is being shown to leave the area.
- » (U) On 20 December, the GOP posted Pastebin messages that specifically taunted the FBI and USPER2 for the "quality" of their investigations and implied an additional threat. No specific consequence was mentioned in the posting.

(U//FOUO) The FBI and DHS are not aware of any specific credible information indicating a physical threat related to these postings. However, the potential remains for GOP or copycat actors to make renewed cyber and/or implied physical threats, to identify new targets, or execute physical attacks if the movie is again scheduled for release. DHS and FBI note that hacking groups have historically made exaggerated threat statements.

(U//FOUO) Federal, state, and local government cyber, counterterrorism, and law enforcement officials, first responders, and private sector security partners are being provided this information and urged to remain vigilant to actual threats of physical violence or cyber attacks.

**(U) Outlook**

(U//FOUO) The GOP's attack on USPER I indicates the increasing willingness of malicious cyber actors to conduct offensive cyber operations against US entities based on perceived injustices or provocations. Though we have seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack—coupled with its coercive nature—sets it apart. The GOP's actions were intended to prevent the public release of a controversial film considered offensive to the GOP. USPER I will release the movie to a limited number of theaters on 25 December. In light of this, cyber intrusions are possible against theaters showing the movie, as well as companies involved in the movie's distribution. The GOP will likely continue to release portions of proprietary data and e-mails stolen from USPER I to keep pressure on USPER I, possibly to get the company to withhold further distribution of the movie, destroy all copies of the film or publicly apologize for its production of "The Interview."

(U) The FBI and DHS stand ready to assist any US company that is the victim of a destructive cyber attack or breach of confidential business information.

**(U) Malware Indicators**

(U) For information specific to recently identified destructive malware, please refer to FBI FLASH message A-00044-MW, dated 1 December 2014, Alert TA 14-353A, "Targeted Destructive Malware," dated 19 December 2014, and DHS/FBI *Joint Indicator Bulletins* numbered 14-20199, dated 9 December 2014, and 14-20199B dated, 15 December 2014.

**(U) Physical Attack Indicators**

(U) Despite a lack of credible physical threat reporting, mass gatherings have historically been attractive targets, and threat actors could view screenings as potentially attractive targets due to the growing media attention. We encourage facility owners and operators, security personnel, and first responders to remain vigilant and report suspicious activities and behaviors that may indicate a potential attack. Some of these behavioral indicators may be constitutionally protected activities and should be supported by additional facts to justify increased suspicions. No single behavioral indicator should be the sole basis for law enforcement action. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

- » (U//FOUO) Persons in crowded areas wearing clothing that is unusually bulky or atypical for the season, possibly to conceal suicide explosives or weapons.
- » (U//FOUO) Persons asking about theater security screening and evacuation procedures without a reasonable explanation.
- » (U//FOUO) Packages—possibly containing explosives—left unattended in open areas or hidden in trash receptacles, lockers, or similar containers.
- » (U//FOUO) Vehicles with sagging suspension or illegally parked near a theater or where crowds gather prior to or following performances and events.
- » (U//FOUO) Vehicles with modifications made, such as hidden compartments or seating removed, to conceal or make room for explosives.

**(U) Report Suspicious Activity**

**(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit <http://nsi.ncirc.gov/resources.aspx>.

**(U) Administrative Note: Law Enforcement Response**

(U//FOUO) Information contained in this intelligence bulletin is for official use only. No portion of this bulletin should be released to the media, the general public, or over nonsecure Internet servers. Release of this material could adversely affect or jeopardize investigative activities.

(U) For comments or questions related to the content or dissemination of this document, please contact the FBI [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov) or the I&A Production Branch by e-mail at [IA.PM@hq.dhs.gov](mailto:IA.PM@hq.dhs.gov).

(U) For comments or questions related to the content or dissemination of this document, please contact the FBI Cyber Intelligence Section, Asia Cyber Intelligence Unit at (703) 633-4591, or I&A Production Branch by e-mail at [IA.PM@hq.dhs.gov](mailto:IA.PM@hq.dhs.gov).

**(U) Tracked by:** HSEC-I.1, HSEC-I.2